WHITE PAPER

5 WAYS TO MANAGE MOBILITY AND IOT RISKS

Reducing network risks by enforcing security policies

aruba
a Hewlett Packard Enterprise company

TechTarget® | Custom Media

INTRODUCTION

Today's workers are more mobile than ever, and there's no end in sight to the growth in connectivity—inside and outside the office. According to Gartner, by 2020, the world will be saturated with more than 21 billion connected devices.[1] Other experts say that by the same year, there will be more people with a mobile phone than those with running water and a car, and that Internet traffic will break the zettabyte barrier.[2]

Clearly, the BYOD security debate is over, as organizations recognized long ago that to stay competitive, they need to be flexible enough to allow users the freedom to connect multiple devices, whether they're owned by IT or not. Most organizations have enabled that flexibility through a measured approach, whereby certain conditions must be met before a user's device can access sensitive data. This includes conditions about the device's status, authentication procedures used, criticality of data being accessed and so on. Mature organizations come up with these requirements based on sound risk assessments and codify them through official policies. These policies are meant to protect the network and data, both in transit and at rest, on mobile and Internet of Things (IoT) devices.

But that's only step one in actually managing risk in this new era of always-on mobile connectivity and IoT initiatives. Policies are only as good as their enforcement mechanisms. And, unfortunately, many organizations don't have the technology or processes in place to actually turn security policies into consistent action, namely through effective and automated enforcement workflows. To truly mitigate the risk of mobile and IoT-enabled data breaches, organizations need to consider the following five steps.

NOTHING ELSE MATTERS UNTIL YOU KNOW WHO AND WHAT IS TRYING TO CONNECT

At any given time, most organizations can't quantify risks because they lack the visibility or controls related to connections to the network. Without this fundamental capability, organizations find it hard to enforce policies inside the network, spot indicators of compromise, and understand how vulnerable they are to new threats derived from mobile users and apps or IoT.

Organizations need an automated way to inventory everything that's connecting to the network as it tries to connect.

This capability should include a way to know:

- Who connects
- How and with which device a user is trying to connect
- Which assets will be accessible to the user's device
- What risks are brought to the table by that particular device or data access permission

DEVICE VISIBILITY NEEDS TO BE PAIRED WITH NETWORK ENFORCEMENT

While the market offers a number of device management tools that provide enterprises a solid look into a device's security status, these tools have their limits. Using mobile device management or endpoint management tools is only one component of a solid mobile security strategy, as they lack the means for actionable network enforcement.

Organizations need the ability to not only inventory which devices are connecting to the network, but also constrain access based on the status of those devices. Organizations need a way to look at contextual information about the device, such as the state of permissions settings within the device, whether the device has been rooted, whether the device has fully updated antimalware software, and whether the device is exhibiting any potential signs of compromise.

Visibility into these contextual elements is a crucial first step. The next step is to pair that with an effective means of network enforcement based on how well the condition of the device matches current security policies. To better protect network assets and prevent attacks from risky devices, organizations need automated access control to ensure that devices that don't meet policy demands cannot connect until they are brought into compliance.

USER AND ENVIRONMENTAL CONTEXT IS CRUCIAL

The more context that goes into access controls, the more fine-grained the policies can be to determine access. Device status is important, but equally important is information about who is putting their fingers on those touchscreens, where these users are connecting from and even what time of day they're connecting.

[1] "Gartner: 21 Billion IoT Devices to Invade by 2020," InformationWeek, Nov. 10, 2015

[2] "Phones Will Drive Internet Traffic Past the Zettabyte Mark This Year," Recode, Feb. 3, 2016

As organizations enforce policies, access control needs to be nuanced enough to gate network assets based on user privileges, location, time of day and more. Additionally, organizations need a way to link multiple devices to a single user and create transparent enforcement processes that keep user context in focus. This same context can then be used to monitor the behavior of both users and entities inside the network.

Ultimately, access control should have automation tuned to the task at hand, using relevant context to minimize mobility-associated risks.

DON'T IGNORE WIRED CONNECTIONS

So much of mobile security today depends on how well organizations secure wireless connections. But organizations shouldn't forget the importance of wired connections.

Unprotected wired ports in public places are quite often an Achilles' heel for an otherwise solid network protection strategy. If a visitor can wander into a public space, unplug a printer or conference room IP phone and plug in a laptop for instant and open access, that's a problem.

HAVE A REMEDIATION PLAN THAT WORKS FOR ANY SCENARIO

Great access control enforcement is one thing, but an organization must have a plan or a workflow in place to solve problems when things go wrong. One of the biggest mistakes organizations make is putting in technology to control device connections to the network but failing to institute an automatic message to users as to why their devices have been restricted from connecting. This kind of oversight swamps help desk workers with trouble tickets, wastes users' time and irritates executives.

As organizations put access controls into place, they'll need a plan and process in place to streamline the workflow after a device has been blocked. This means automatically triggering remediation, if possible. It means informing users of the problem that has caused a restriction. It means engaging help desk and IT support. And it means providing the documentation or other resources necessary to walk users through remediation as swiftly as possible.

HOW ARUBA CLEARPASS HELPS

ClearPass offers the visibility, policy control, workflow automation and integration with other security products necessary to put these five steps into action. Features include:

- Built-in profiling that collects real-time data such as device categories, vendors and operating system versions.
- Authentication processes that allow for the utilization of user and device context for enforcement.
- Context sharing that works with third-party systems. Such systems include firewalls, endpoint management, user and entity behavior analytics, device management and IT services that offer accurate data about users and devices to improve remediation workflows.

These capabilities give organizations the power to enforce how users and devices use internal resources, regardless of a user’s role, device type or location from which a connection is being established.

CONCLUSION: PUTTING IT ALL TOGETHER

As organizations endeavor to take all of these steps toward reducing mobile risks, there’s no single technological magic wand. Organizations need a well-balanced ecosystem of controls to address all of the dimensions of risk. They must consider that they’ll need to pair granular network access controls and visibility of connections with IT orchestration platforms for remediation.

To do this, organizations must deploy solutions with integration top of mind, ensuring that the vendors they choose will work well together for a seamless security backstop.